REMARKS

Applicants have carefully considered the April 7, 2006 Office Action regarding the above-identified application. Claims 9-16 have been cancelled to reduce issues. Independent claims 1 and 17 are amended to more clearly distinguish over applied art, and a few of the dependent claims have been revised to match the amended independent claim language. Also, a grammar error has been corrected in the third line of claim 5. The amendments to the claims above and the remarks that follow are presented in a bona fide effort to respond thereto and address all issues raised in that Action. Prompt favorable reconsideration of this amended application is requested.

Summary of the Latest Art Rejections

The April 7, 2006 Office Action rejected claims 1-4, 6, 8-12, 14, 16-19 and 21 under 35 U.S.C. §103 as unpatentable over U.S. Patent No. 6,192,361 to Huang in combination with U.S. Patent No. 6,476,833 to Moshfeghi.

Claims 5 and 13 stand rejected under 35 U.S.C. §103 as unpatentable over Huang and Moshfeghi, further in view of U.S. Application Publication No. 2002/0198829 to Ludwig et al. (hereinafter Ludwig).

Claims 7 and 15 stand rejected under 35 U.S.C. §103 as unpatentable over Huang and Moshfeghi, further in view of U.S. Patent No. 6,029,160 to Cabrera et al. (hereinafter Cabrera).

These rejections are traversed.

Patentability

It is respectfully submitted that none of the combinations applied in the latest art rejections actually meets the recited requirements of the independent claims. Hence, the claims

should all be patentable over the art. Detailed explanations of patentability follow, first with respect to the system claims and then with respect to the method claims.

System Claims 1-8

As amended above, independent claim 1 recites a storage system that comprises a storage device for storing data files to be accessed by one or more users and a storage management system for managing the storage device. The storage management system includes a storage configuration information file, which contains settings of the storage system with respect to operation of the storage device.

Support for this amended claim scope appears for example on application page 6 (lines 3-28) and application page 7 (lines 1-10). In the example discussed on pages 6 and 7, the storage system 101 includes a storage device 100, such as a disc drive with a large storage capacity for users' data, and a management mechanism for managing the large capacity of data in response to an instruction from a manager 109. The disclosed management mechanism of the storage system 101 is a service processor (Fig. 1), which implements software-based control of manager access to the storage system 101 via the network 500. A storage configuration information file 106, which contains configuration information, is stored on storage control mechanism. Examples of this configuration information include information for the data files or discs in the storage system 101 and information on the connection states of storage data users or a host computer to be connected to the data files or discs. Rewriting the configuration information in file 106 alters settings of the system configuration, for example, with respect to the disc(s), users and/or host computer.

As recited in independent claim 1, the storage management system comprises a management object for controlling management access in response to a request from a manager;

the storage configuration information file containing the settings of the storage system with respect to the operation of the storage device; and a temporary software interface object for accessing the settings in the storage configuration information file through the network. The management object controls management access by authenticating a manager's ID and password in response to a request from the manager. When the manager is authenticated, the management object creates the temporary software interface object for accessing the settings in the storage configuration information file through the network. The temporary software interface object expires after a predetermined permission time.

The authenticated manager's access to the settings contained in the storage configuration information file is permitted only while the temporary software interface object exists, that is to say between creation and expiration thereof. The management object transmits a key, needed for communication through the network with the temporary software interface object, to the authenticated manager to enable management access to the storage configuration information file. The temporary software interface object that permits the manager to access the settings in the storage configuration information file is erased after lapse of the predetermined permission time, so as to expire access by the authenticated manager.

The combination of Huang and Moshfeghi applied to reject independent claim 1 does not disclose or teach a storage system of the type now recited in claim 1.

Huang is actually directed to controlling access to a switching system. As such, Huang does not disclose a storage system, and the disclosed access control is not implemented as part of a storage management system.

In Huang, the full group privileges access mechanism contains storage files which store information related to authorized users. The system manager building block in combination with

the system security manager client building block and the system security manager server building block can access the storage file information related to the authorized users in order to determine whether, and to what extent, users can access the telecommunications switching system. Attention, for example, may be directed to the abstract of the Huang patent. Such files that the mechanism itself uses to determine whether, and to what extent, users can access the telecommunications switching system are quite different from data files to be accessed by one or more users, as contained in the storage device in the storage system of claim 1.

The rejection identified the description running from column 8, line 64, to column 9, line 6 for a disclosure of a system configuration file. However, the text in question reads:

> System Management Interface 56 and Servers 60, in conjunction with GUI Launcher 8, permit users to access and communicate with the Telecommunications Switching System 230 for purposes such as the test and reconfiguration of the Telecommunications Switching System 230, as well as the monitoring of Telecommunications Switching System 230's performance, faults and security system. Users may use Remote Computer 10 to send commands and messages to the Telecommunications Switching System 230, as well as to receive commands and messages therefrom.

As such, the configuration disclosed by Huang is that of a switching system. It is not a storage configuration information file containing settings of the storage system with respect to operation of the storage device, as recited in claim 1. Allowing an access to the switching system configuration in Huang does not satisfy claim requirements regarding allowing an authenticated manager to access a storage configuration information file containing settings of the storage management system with respect to operation of the storage device.

In addition to the above noted aspects relating to a storage system and a related system configuration file, Huang fails to teach the creating and erasing of a temporary software interface object that is part of the storage management system, as required by claim 1. Huang discloses using a time limit for access, in which permission expires if a user is inactive for a predetermined

period (text at column 15, lines 39-49, as cited in the rejection). An inactivity period alone is not enough to meet the creation and erasure requirements of claim 1. The rejection also cited the text in column 7, lines 59-67. The cited paragraph, beginning in line 59 of column 7, states in its entirety:

> When the user of Remote Computer 10 wishes to terminate the logon session, the user enters the appropriate command at Remote Computer 10, and the GUI Launcher sends a message instructing System Manager 18 to terminate the session, as shown in Block 52. When the logon session has been terminated, Remote Computer 10 does not retain Java Applet 22. Rather, for the next logon session from Remote Computer 10, Remote Server 14 again provides to Remote Computer 10, typically in the form of a Java Applet 22, the application program which enables Remote Computer 10 to communicate with the Telecommunications Switching System 230. This eliminates the need to install and maintain multiple copies of the necessary application program on one or more Remote Computers 10. Instead, the necessary application program need only be installed, maintained and updated on Remote Server 14.

Apparently, the server of Huang provides a Java applet to the permitted user's computer for a session, and that computer does not retain the applet after the session is terminated. However, as taught by Huang, that applet is in the remote computer. Applicants' claim 1 recites a temporary software interface object as an element of the storage management system, that is to say in the storage system itself. In the example disclosed in the specification, the interface object software is a remote management interface (RMI) object 107 created by the remote invocation interface 108 (see e.g. page 7, lines 4-21). The object 107 is dynamically generated and expired or erased (see e.g. page 6, lines 15-22). A teaching to provide an applet to a remote computer and that the applet need not be retained after a session terminates (Huang) does not satisfy the claim requirements for creating and erasing the temporary software interface object, that is to say an element of the storage management system itself.

From the discussion above, it should be clear that the Huang document does not satisfy the claim requirements regarding a storage system, a storage device, a storage configuration

information file containing settings of the storage system with respect to operation of the storage device and creating/erasing a temporary software interface object for accessing the settings in the storage configuration information file. In the rejection, the Examiner acknowledges that Huang also fails to satisfy the claim requirement that the management object transmit a key, needed for communication through the network with the temporary software interface object, to the authenticated manager to enable management access to the storage configuration information file. The 103 rejection cited Moshfeghi for support of the conclusion that addition of such key transmission to the system of Huang would have been obvious. Even if such a combination were obvious, the system of Huang modified to add key transmission ala Moshfeghi would still not meet the claim requirements regarding a storage system, a storage device, a storage configuration information file containing settings of the storage system with respect to operation of the storage device and creating/erasing a temporary software interface object for accessing the settings in the storage configuration information file. Since the combination proposed in the rejection of claim 1 would not meet the requirements of that independent claim, the claim should be patentable over Huang and Moshfeghi.

The teachings that the later rejections identified in secondary document citations to Ludwig and Cabrera do not address the deficiencies of the basic combination of Huang with Moshfeghi. The Action cites Ludwig for a teaching to disable accounts after a predetermined time of inactivity. The Action cites Cabrera for a teaching to use a flag to temporarily stop use of objects in response to maintenance. It is respectfully submitted that the applied combinations of (1) Huang and Moshfeghi with Ludwig and (2) Huang and Moshfeghi with Cabrera still would not meet the above discussed requirements of independent claim 1. Hence, claim 1 and

all of its dependent claims (including claims 5 and 7) patentably distinguish over these additional combinations.

It is respectfully submitted that, for reasons stated above, none of the applied combinations renders any of the claims 1-8 unpatentable over the art. Hence, all of the art rejections from the April 7, 2006 Office Action should be withdrawn with respect to the system claims.

Method Claims 17-19 and 21

Independent claim 17 is a method claim. As amended, the first step of the method is providing user access to data files stored in a storage device of a storage system. The provision of access is based at least in part on settings of the storage system contained in a storage configuration information file in a storage management system. Support for the amended claim language should be readily apparent from application pages 6 and 7 and application Fig. 1. The Huang document does not disclose this step. Huang is actually directed to controlling access to a switching system. Huang allows a user to access a configuration of the switching system. The configuration disclosed by Huang is that of a switching system, not a storage configuration information file containing settings of a system, as in claim 17. Hence, Huang does not provide user access to data files stored in a storage device of a storage system based at least in part on settings of the storage system contained in a storage configuration information file in a storage management system.

The method of claim 17 involves authenticating a manager, and in response, creating a temporary software interface object at the storage management system for the authenticated manager. This object is necessary for accessing the storage system settings contained in the storage configuration information file through the network. The authenticated manager's access

to the settings contained in the storage configuration information file is permitted only while the temporary software interface object exists. The method includes a step of transmitting a key needed for communication through the network with the temporary software interface object to the authenticated manager, to enable management access to the storage configuration information file. The temporary software interface object is erased after a lapse of a predetermined permission time, so as to expire the authenticated manager's ability to access the settings in the storage configuration information file. Huang does not disclose these steps.

Huang discloses using a time limit for access, in which permission expires if a user is inactive for a predetermined period (text at column 15, lines 39-49, as cited in the rejection). Huang also teaches providing a Java applet to the permitted user's computer for a session, and that computer does not retain the applet after the session is terminated (column 7, lines 59-67, as cited in the rejection). As taught by Huang, that applet is in the remote computer. Such a methodology does not satisfy the method claim requirements regarding steps of creating and erasing the temporary software interface object at the storage management system.

The combination of Huang and Moshfeghi applied to reject independent claim 17 does not fairly suggest such a methodology for controlling manager access to storage system settings in a configuration information file.

From the discussion above, it should be clear that the Huang document does not satisfy the claim requirements regarding providing user access to data files stored in a storage device of a storage system based at least in part on settings of the storage system contained in a storage configuration information file in a storage management system, creating the temporary software interface object at the storage management system to enable access to the system settings in the storage configuration information file or the erasing of that temporary software interface object

after a lapse of a predetermined permission time. In the rejection, the Examiner acknowledges that Huang also fails to satisfy the claim requirement for a step of transmitting a key, needed for communication through the network with the temporary software interface object, to the authenticated manager to enable management access to the storage configuration information file. The 103 rejection cited Moshfeghi for support of the conclusion that addition of such key transmission to the method of Huang would have been obvious. Even if such a combination were obvious, the methodology of Huang modified to add key transmission ala Moshfeghi would still not meet the claim requirements regarding providing user access to data files stored in a storage device of a storage system based at least in part on settings of the storage system contained in a storage configuration information file in a storage management system, creating the temporary software interface object at the storage management system to enable access to the system settings in the storage configuration information file or the erasing of that temporary software interface object after a lapse of a predetermined permission time. Since the combination proposed in the rejection of claim 17 would not meet the requirements of that independent claim, the claim should be patentable over Huang and Moshfeghi.

The teachings that the later rejections identified in secondary document citations to Ludwig and Cabrera do not address the deficiencies of the basic combination of Huang with Moshfeghi. As noted earlier, the Action cited Ludwig for a teaching to disable accounts after a predetermined time of inactivity; and the Action cited Cabrera for a teaching to use a flag to temporarily stop use of objects in response to maintenance. Such modifications of the combination of Huang and Moshfeghi still would not meet the above discussed requirements of independent claim 17. Hence, claim 17 and all of its dependent claims (including claim 15) patentably distinguish over the additional combinations with Ludwig and Cabrera.

It is respectfully submitted that, for reasons stated above, none of the applied combinations renders any of method claims 17-19 and 21 unpatentable over the art. Hence, all of the art rejections from the April 7, 2006 Office Action should be withdrawn with respect to the method claims.

Conclusions

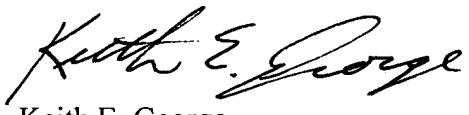
Upon entry of the above claim amendments, claims 1-7, 17-19 and 21 are active in this application, all of which should be patentable over the art applied in the latest Office Action. It is submitted that all of the claims are in condition for allowance. Accordingly, this case should now be ready to pass to issue; and Applicants respectfully request a prompt favorable reconsideration of this matter.

It is believed that this response addresses all issues raised in the outstanding Office Action. However, if any further issue should arise that may be addressed in a further interview or an Examiner's amendment, it is requested that the Examiner telephone Applicants' representative at the number shown below.

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8603 KEG:apr
Facsimile: 202.756.8087
Date: May 22, 2006

Please recognize our Customer No. 20277 as our correspondence address.